Physical Education, Health and Social Sciences

https://journal-of-social-education.org E-ISSN: 2958-5996

P-ISSN: 2958-5988

The Language of Deception: How Hackers and Scammers Exploit Urgency-Driven Terminology, Trust Based Phrasing, and Authoritative Expression in Digital Fraud

Neha Rubbab Butt[1], Aresha Chaudhry[2], Mehar Jan[1], Maha Hijab Sikandar[3]

[1] BS Hons (English Literature), University of Management and Technology.

[2] MPhil (English Linguistics), University of Central Punjab.

[3] PhD Scholar (English Linguistics), Riphah International University.

DOI: https://doi.org/10.63163/jpehss.v3i4.912

Abstract

In the digital age, language plays a powerful role in shaping human behavior online. Scammers have learned to exploit linguistic cues to manipulate users and commit fraud, making it essential to understand how language is used as a tool in cybercrime. With the growing prevalence of online scams, this report aims to raise awareness and propose preventive strategies by examining the linguistic techniques behind digital fraud. Despite advancements in cybersecurity, users continue to fall victim to scams due to the persuasive and manipulative language used in fraudulent messages. There remains a limited understanding of the specific patterns that trigger trust, urgency, or fear, making users especially vulnerable. To explore this, we analyzed real-life scam messages from emails, texts, and social media platforms, and conducted a brief survey to assess user awareness of deceptive language. The data revealed recurring strategies such as the use of urgency ("act now"), fear ("account suspended"), and false authority ("official notice") to provoke immediate reactions. Scammers also utilize visual elements like logos and formal formatting to enhance credibility. Survey responses showed that many users overlook red flags due to the professional tone and structure of these messages. Our findings suggest that language is a central factor in the effectiveness of online scams. By educating users about these tactics and encouraging critical thinking, we can reduce their impact. Furthermore, we recommend incorporating language-based alerts into digital communication systems as a proactive defense against cyber fraud.

Keywords: Digital fraud; Linguistic manipulation; Deceptive language; Urgency; Trust; False authority; Online scams; Cybercrime; User awareness.

1. Introduction

This paper summarises the results of our research group's work on investigating how language in online communication can be used to commit fraud, manipulate users, and exploit psychological triggers. The introduction provides the project background description, outlines the scope of our research, and briefly describes the document organisation.

With the advent of the digital era, internet platforms have transformed social interactions, service access, and financial transactions. However, it has also brought with it the scope for digital fraud, with hackers and scammers employing elaborate methods to deceive unsuspecting individuals. Manipulation of language is one of the most common methods. Using urgency-based language,

trustworthy language, and authoritative statements, scammers use psychological stimuli to make a person have a sense of urgency, trustworthiness, and expertise.

Studies have indicated that scammers employ such linguistic tactics to create legitimacy and force victims to make quick choices, leading to identity theft and financial loss. Scammers and hackers design messages to create a sense of urgency, create false trust, or assume an authoritative tone, all for the purpose of forcing victims to disclose confidential information, make impulsive financial choices, or unknowingly participate in criminal acts. Urgency-driven terminology creates a sense of urgency that causes people to act without full consideration of the implications. Trust-based phrasing attempts to use the victim's sense of comfort and security to make the victim susceptible to the fraud. Lastly, authoritative expression uses perceived expertise and legitimacy to trick victims into believing the scammer's message.

This research is centred on the linguistic and psychological tactics used by swindlers in online deception, namely how the use of urgency words, trust phrases, and authoritative speech is utilised to swindle and take advantage of people. The findings of this study aim to contribute to the ongoing efforts to safeguard users from digital fraud by providing a deeper understanding of the role of language in manipulation and deception.

The above pie chart illustrates the response to the question: "Have you ever responded to a suspicious message because the wording made it seem to be trustworthy or urgent?" The figures show that 72% of the respondents have responded to a suspicious message because it seemed to be trustworthy or urgent

.

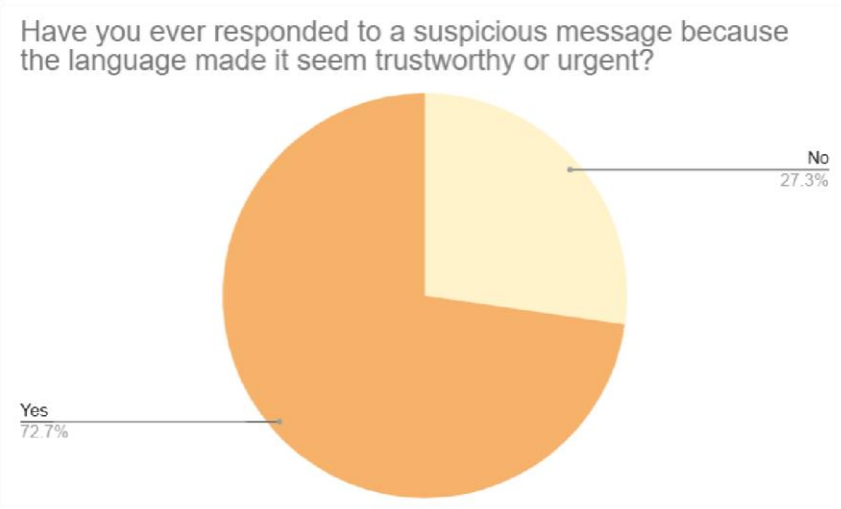


Figure 1: Respondents' Reactions to Suspicious Messages Based on Language

As much as the incidence of such fraud has been on the rise, there is limited research on how exactly language influences victims' decision-making in digital fraud. This research attempts to discover how fraudsters utilise these three particular forms of language urgency, trust, and authority, and to what degree they render people more vulnerable to digital fraud.

1.1.Problem Statement

Cybercrime is a rapidly expanding phenomenon, resulting in billions of dollars lost each year due to web scams. Although much emphasis has been placed on the technological aspect of hacking and scam tactics, relatively little has been placed on the psychology and linguistic manipulation behind many internet-based scams. Scammers often use language to manipulate, bluff, and persuade victims, using urgency, trust, and authority to create a sense of security or to push victims

into impulsive decisions. Language is an extremely powerful tool of deception, enabling scammers to construct plausible narratives with human emotions and cognitive shortcuts. Understanding how these linguistic tactics influence victims' behaviour is crucial in developing effective preventive measures and educational campaigns aimed at reducing digital fraud.

1.2. Research Objectives

● To identify the particular linguistic strategies used by scammers and hackers in cyber fraud, that is, urgency-based language, words of trust, and claims of authority.
● To investigate how linguistic cues, i.e., urgency, credibility, and authority, influence individuals' decision-making and guide them to their vulnerabilities when they receive insincere digital messages.
● To investigate how the manipulation of language is linked to the possibility of being scammed online.

1.3. Research Questions

1. How do urgency-created language, trust-based wording, and commanding phrasing in online messages affect people's vulnerability to online fraud?
2. What are the most prevalent linguistic patterns used by scammers to exploit trust and trigger immediate action in fraudulent online messages?
3. How does the tone in a scam message influence a receiver's compliance or reaction to the message?

1.4. Purpose of the Study

With the rise of digital scams through emails, text messages, and widespread social media, there is a growing need to understand the linguistic strategies scammers use to manipulate language. Language has become a powerful tool in the hands of scammers, who utilise specific tones, word choices, and rhetorical techniques to build trust and create a false sense of urgency. Our project explores how certain tones, word choices, and rhetorical methods are employed to manipulate trust in scam messages, ultimately deceiving individuals with carefully crafted and critically manipulated language. By analysing these strategies, we aim to raise awareness and suggest ways to improve scam detection. Additionally, through this research, we intend to highlight how language can be exploited for manipulative ends and propose practical methods to identify and counter such scams.

1.5. Scope of the Study

Its focus was on the analysis of linguistic strategies, specifically, urgency-based wordings, trust-based wordings, and authoritative speech, found in fraudulent online messages. It explored the way the language influences an individual's decision-making and emotional responses and the resulting susceptibility to scams.
Furthermore, the study will constitute a valuable contribution to students, educators, and the general public by sensitising them to the psychological manipulation of fraudulent online communication. Through the identification of how particular linguistic signs cause spontaneous or compliant behaviour, the study aims to promote more cautious and informed online interaction. The study will also be beneficial to future researchers by providing the basis for further studies on the intersection of language, psychology, and cybersecurity within the context of cyber fraud. The study can also be applied in the design of educational resources and prevention strategies to promote digital literacy and scam resilience.

2. Literature Review

The prevalence of cybercrime and online fraud has led to great concern regarding the tactics employed by cybercriminals in defrauding victims. Among the most significant elements of cyber deception is the vocabulary hackers and scammers employ in leading people astray. This literature review explores how urgency-driven terminology, trust-based phrasing, and authoritative expressions are employed in the language of deception to exploit psychological vulnerabilities.

2.1. Urgency-Driven Terminology

Urgency is a powerful psychological urge usually used in scam messages to generate immediate action by the victims. Scholars have explored how con artists usually employ words which evoke a sense of urgency of time, for instance, "Immediate action required," "Limited time offer," and "Your account will be suspended soon." These are threatening words that are intended to scare and intimidate, resulting in individuals making impulsive decisions without due caution. Urgency creates an emotional reaction that obscures reason and forces one to react impulsively.

A study by Johnson and Stephens [A] highlights that urgency-induced language significantly reduces the cognitive effort required to assess the legitimacy of an offer. Spammers capitalise on this with a high-stress environment where victims are asked to react impulsively. Impostors issue a threat of immediate harm or time urgency through the use of words like "urgent," "immediate action required," or "limited supply." These words evoke a false sense of urgency, leading victims to act without consideration of the whole picture.

One of the most prevalent and successful linguistic tools employed in online scams is urgency-driven terminology. An excellent example here is the message: "Your account will be suspended within 24 hours unless you confirm now." This type of language is intended to inspire fear and compel the recipient to act without analysing the truthfulness of the message. The artificially created time limit ("24 hours") creates a feeling of impending consequence, while the "verify now" mandate echoes the phrasing of an official order.

All these reduce the likelihood that the user will pause to learn more or a trusted source. There is evidence that under time pressure, decision-making can be seriously compromised, especially in online environments where users expect instant returns and real-time communication. A sample example is provided below to illustrate how such a message can appear in a phishing email or message, illustrating the tone, styling, and language used to enhance credibility and pressure.

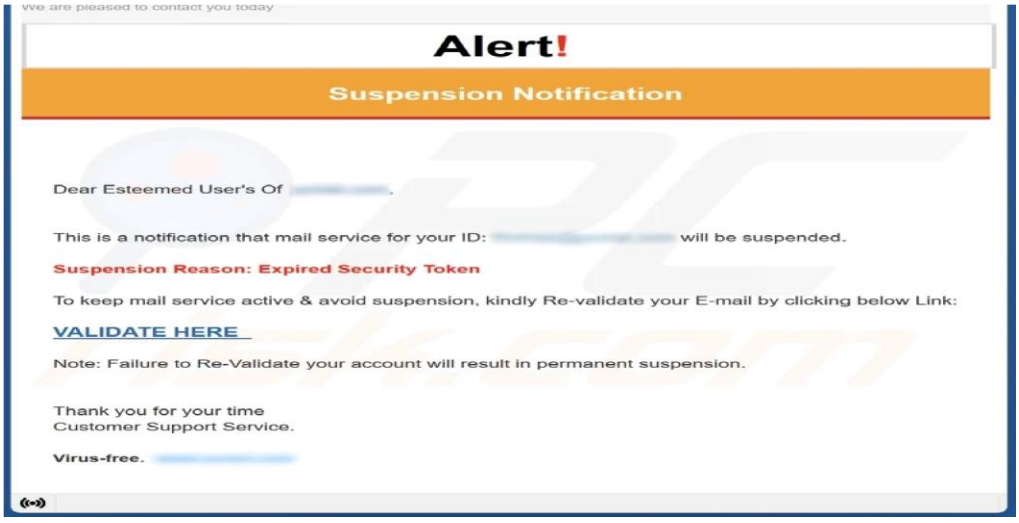


Figure 2: Example of a phishing message using urgency-driven language. Adapted from (mukti, 2024)

Similarly, Jimmy (Jimmy, 2024) found that urgency, when coupled with a demand for personal information, increases the likelihood of individuals falling victim to phishing attacks. The manipulation of time sensitivity plays a key role in increasing the effectiveness of fraudulent messages, pushing individuals to act quickly and without verification.

2.2. Trust-Based Phrasing

Trust is another tool utilised in fraudulent digital communications. Words that mimic the voice of trusted institutions are typically used by scammers. Studies have shown that victims are more likely to be victimised by fraudulent schemes if they think that the source is trustworthy. Trust-based words are intended to make the victim feel safe, a false sense of security. By mimicking the tone, style, and voice of these trusted institutions, scammers craft a message that appears authentic and authoritative.

Daudi (Daudi, 2024) illustrate that such language is particularly effective in phishing because it exploits pre-existing trust in organisations such as banks, government departments, and corporations. The psychological dynamic of trust is used in the strategy since people tend to react more favorably to messages that are seen as familiar or from purportedly trusted sources. Personalised language and the use of familiar names, logos, or allusions to the victim's presence enhance the success rate of the scam.

Scammers can imitate and replicate the communication patterns of authentic parties, thus creating perceived legitimacy of spurious messages (Lauren E. Scissors, 2008). Coupled with pressure, scammers employ trust-based framing to influence the perception of legitimacy by the victim. Trust-based deception exploits the cognitive bias of the victim towards trusting familiar sources.

The second strategy that is often used by scammers is trust-based wording and enticing rewards, like in this message: "Take an Amazon survey and get an exclusive reward." This scam exploits the recognition and goodwill of a reputable brand like Amazon to create a false sense of security. By offering an "exclusive reward," the message hooks the user's reward motivation and frames the offer as a time-limited offer.

The language is often casual and friendly, mimicking real promotional emails to reduce suspicion. Victims are typically asked to click a link and answer a few harmless-looking questions, after which they are prompted to enter personal information or payment details to "claim" the prize. In reality, the survey is fake, and the information collected is used for phishing or financial fraud. The combination of a well-known brand name and the promise of a reward is highly effective at lowering users' defences, especially when paired with urgency (“limited time offer”) or social proof (“many users have already claimed their gift”).

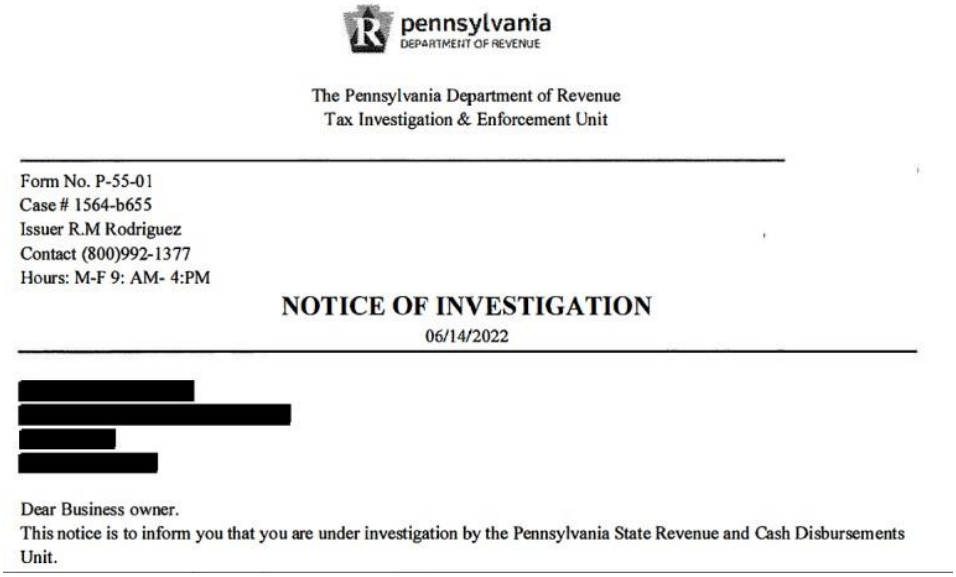
Figure 3: Example of a deceptive message impersonating Amazon, offering an "exclusive reward. Adapted from (Kutub Thakur, 2023)

2.3. Authoritative Expression

The authoritative tone in scam messages is designed to manipulate the victim into compliance by presenting the scammer as an expert or an official figure. Phrases like “Failure to comply may result in legal consequences” or “This is a mandatory procedure” create a sense of authority and pressure the victim to act without questioning the source. Many scam messages adopt the language of officialdom, using formal terminology, legal jargon, or commands that make the message appear as if it originates from a figure of power. By imbuing the message with a sense of authority, scammers create psychological pressure on the victim to comply.

Social psychology studies have illustrated that individuals are likely to follow perceived authority figures, even in the absence of proper verification. Carter (Carter, 2023) argues in his study that the language of authority exploits the human tendency to follow perceived authority figures, particularly in high-stakes or foreign settings. Scammers will present themselves as government agents, police officers, or corporate executives, and in so doing, exploit the social compliance norm with authority.

Spammers frequently exploit authoritative expressions in their fraudulent notices, pretending as trusted institutions such as banks, government agencies, or corporations. One example is a notice given in the format of an official notice, for instance: "Action required immediately: Your account has been flagged for suspicious activity. Failure to act will result in account suspension." The notice uses authoritative language, implying the user is being investigated by a valid authority. The official tone and structure, typically mimicking the style of genuine notices, create a sense of urgency and fear. Victims take the notice literally and may easily oblige the request, revealing sensitive information or following links to phishing websites. Below is a visual representation of such a fraudulent notice, which illustrates how spammers misuse the authority of institutions to deceive and exploit users.



pennsylvania
DEPARTMENT OF REVENUE

The Pennsylvania Department of Revenue
Tax Investigation & Enforcement Unit

Form No. P-55-01
Case # 1564-b655
Issuer R.M Rodriguez
Contact (800)992-1377
Hours: M-F 9: AM- 4:PM

NOTICE OF INVESTIGATION

06/14/2022

[redacted]

Dear Business owner.
This notice is to inform you that you are under investigation by the Pennsylvania State Revenue and Cash Disbursements Unit.

Figure 4: Example of a fraudulent message impersonating an official notice.Adapted from (Company, 2022)

In addition, these scammers often use threats of institutional or legal power to make themselves seem legitimate. This was also explored by Suela (Suela, 2024), and it was found that scams threatening legal action were more likely to elicit financial transactions than more casual

fraudulent requests. This manipulation of power is effective as a combination with other psychological cues, like urgency or trust, to further convince the victim that the message is real.

2.4. Combination of Techniques in Scam Communication

Spammers often combine these linguistic strategies to maximise their effectiveness in their scams. A message may start as a threat of urgency, follow with trust-based phrasing, and conclude with a demand framed in authority. This tri-layered message intensifies the psychological pressure put on the victim, reducing the victim's capacity to evaluate the message critically. The convergence of urgency, trust-based phrasing, and authoritative tone within scam messages forms a powerful three-piece combination that makes the message more effective.

Studies conducted by Lawson et.al (Lawson, Zielinska, Pearson, & Mayhorn, 2017) and Liu (Liu, 2024) show that these hybrid communication tactics are most successful in the case of text message fraud and email fraud, where the victim has a limited attention span. These tactics are used in combination to produce a believable and manipulative message that circumvents usual cognitive defences.

By combining these factors, scammers evoke both the mental and emotional reactions of victims, making it far more likely that they will respond without carefully considering the situation. The brief, concise nature of scam messages typically mimics authentic communications from banks, computer companies, or government agencies, further lending to their apparent authenticity. Furthermore, the visual nature of such messages, large text sizes, capitalised letters, or official logos also lends credibility to them. Victims might lack the time or technical knowledge to authenticate the sender, particularly when they are under pressure. Consequently, this combination of visual and emotional effect considerably boosts the likelihood of interaction, making it an extremely powerful tool for scammers in the era of the internet, leading users into traps, and scammers to benefit from it. This combination not only increases the emotional effect of the message but also makes it credible.

This layered use of words as a strategy exploits emotional buttons such as fear, urgency, and trust and gets people to react emotionally rather than rationally. The scammers, for example, may begin with words that trigger a sense of urgency, such as "Immediate action required", to capture the attention of the victim in a hurry. This is then followed by trust-evoking words, where the message adopts the tone and voice of an authentic organisation such as a bank or government department, thereby evoking a sense of familiarity and authenticity. The message may then conclude with words of authority, such as the use of legal jargon or directives from a commanding voice, forcing the victim to comply without questioning the directive.

The use of urgency-induced phrases such as “act now” or “limited time offer” and trust-building techniques, including posing as official bodies, frequently creates a grey area between legitimate and scam communication and contributes towards making it harder for people of all ages to spot scams. Regardless of the age, the psychology behind these scams, whether it’s the urgency-based language, trust-based language or the authoritative language, is going to have an effect on the recipients and possibly cause them to act impulsively. As Figure 5, sourced from Scamwatch, indicates, scams are reported from every age group, meaning that all demographics are vulnerable to these misleading methods.

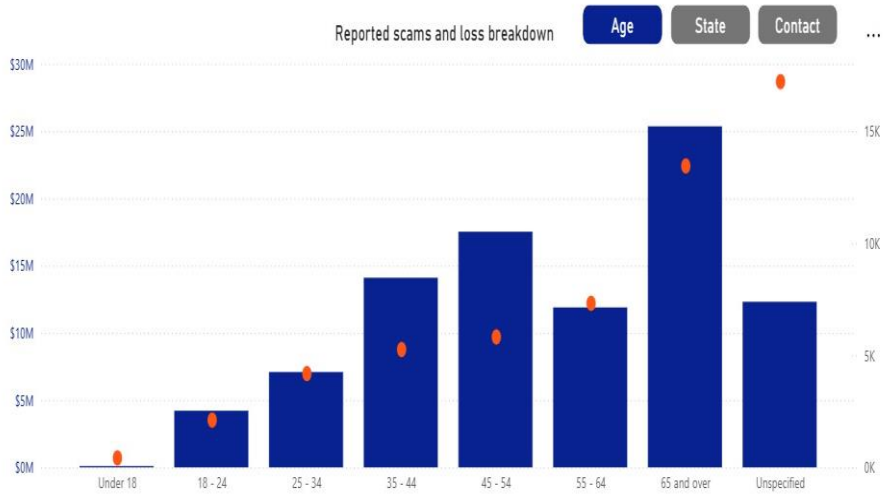


Figure 5: Scam reports by age group, adapted from Scamwatch (Scamwatch, 2024)

Scams target people of all ages, and different age groups may have different vulnerabilities to particular scams. More tech-savvy younger people may be targeted with scams through the internet and social media, while older people might be swindled through old-school scams like phone-based con games or phishing-type scams that afflict people of all ages, who also display different vulnerabilities to these scams. Victims of scams, Scamwatch data indicates, occupy a broad demographic, illustrating the extent of online fraud across all ages. The distribution of scam reports by age group also demonstrates that individuals of all ages are susceptible to scams and includes less traditional forms of scam reports, like online and social media scams for younger people and phone fraud or phishing for older people.

Although prior work has analysed linguistic tactics adopted by scams but efforts have not been made to understand how the tactics are underlined and interact to maximise the success potential. This research seeks to contribute to this gap by analysing actual scam messages and investigating the role of urgency, accused trust and authority in the decision-making process of victims. Using questionnaires, surveys and interviews with scam victims, the research will investigate the psychological impact of manipulative language. With the digital world still developing, there will be a need for anti-scam efforts for research in the language features and cybercrime to reduce the effects and help protect targeted and susceptible users.

3. Methodology

This study investigates how language operates in digital fraud, focusing on the manipulation tactics employed by hackers and scammers. To understand the influence of urgency-oriented vocabulary, trust-focused wording and authoritative language on the victims' decision-making behaviour, we utilised a questionnaire to gather data and carried out a survey in which we examined survey responses for distinct patterns and trends.

3.1. Questionnaire

Appendix A describes the content of the survey questionnaire, which was designed to collect information regarding individuals' attitudes and experiences involving digital fraud (namely, scam-communicating language). Our survey included 10 questions, which we designed to examine which types of language manipulations in fraudulent messages (e.g., creating urgency, establishing trust and authority) affect people's responses to them.

The questionnaire was comprised of questions that measured awareness, knowledge and experience of online fraud. First, it tested how familiar the fraudsters familiarity with various kinds

of scams, phishing, fraudulent ads and social engineering methods. Second, we addressed how participants perceived particular language features like urgency, trust and authority, by having them judge example messages of scams employing these strategies. Lastly, it tested if participants were fraud victims previously and the influence of the message language on their decision to participate.

3.2. Research Design

The survey consisted of both closed and open-ended questions to provide a quantitative measure of awareness and a qualitative understanding of respondents' experiences. A Likert scale was used for many questions using a five-point scale containing Strongly Disagree = 1, Disagree = 2, Not sure =3, Agree = 4 and Strongly Agree =5 so that the respondents could choose the option which best supports their opinion allowing participants to rate their agreement with statements related to the urgency, trust, and authority of scam messages. The research combined qualitative analysis of scam messages with quantitative survey data to provide a comprehensive understanding of the topic.

3.3. Population

The population for this study includes all individuals who have experienced exposure to online fraudulent messages, such as scam emails, phishing texts, and deceptive advertisements. This broad group represents the target audience affected by trust-based manipulation tactics across various digital platforms. By focusing on this population, the study aims to understand general patterns in language exploitation and how different demographics respond to manipulated communication strategies.

3.4. Sample

Given the extensive size of the target population, a sample was selected to conduct the study effectively. The sample includes 200 individuals (aged 18–45) recruited by online questionnaires and the promotion on social media. Attempts were made to recruit participants who varied in age, gender and digital skills. By examining the responses of these respondents, the study aims to develop insights that generalise to patterns of susceptibility to trust manipulation in the context of deceptive email communication.

3.5. Data Analysis

The data was analysed by using both quantitative and qualitative methods. For the quantitative analysis, we employed descriptive statistics to summarise the participants' responses. We calculated the mean, median, and mode for Likert scale questions to determine general trends in the perception of scam language.

To further analyse the relationship between specific linguistic tactics (urgency, trust, authority) and participants' likelihood of falling victim to scams, we used pie charts and graphs for data visualisation to identify patterns and trends within the data to understand how significantly scammers were affecting users.

For the qualitative analysis, responses to open-ended questions were categorised using thematic analysis. We identified recurring themes related to the linguistic strategies participants found most persuasive in scams. This helped us to understand how language affects individuals' susceptibility to digital fraud beyond just statistical measures.

3.6. Ethical Considerations

This study was conducted in full compliance with ethical guidelines for research involving human

participants. Before participation, all individuals were informed about the purpose and voluntary nature of the study through an introductory statement at the beginning of the survey. The survey was designed to be anonymous; no names, addresses or other identifying information were gathered. We accessed the data for academic purposes only, and confidentiality was maintained in a secure place. The participants were also informed about their right to discontinue at any time without giving any reason, as well as without any prejudice, to respect autonomy and avoid any distress.

4. Results and Findings

As digital communication becomes more and more integrated in our daily lives, cybercriminals are no longer relying solely on technical exploits; rather, they have turned to ways of manipulating human behaviour through language. This section discusses the findings on scam messages and surveys, focusing on the way in which particular linguistic manipulations are perceived and their effect on behaviour. By considering urgency-laden language, trust-building wording and power-positioning tones, we aim to show why and how these components particularly constitute the success of digital fraud and the susceptibility of persons in cyberspace.

4.1 Urgency-Driven Terminology

Scammers frequently leverage urgency to try to pressurise recipients to respond immediately without critically engaging with the contents of the message. Use of urgency-focused words is a psychological tool that works on individuals who are moved to act based on emotions of FEAR, anxiety or Excitement. Phrases like "You are the winner of Lotto" and "Contact our claims agent urgently," for example, are coated to sound like crises. These sentiments are also similar to real-time sensitive alerts, which means that scammers are very successful in fooling users. The general tenor is authoritative and imperative, allowing for little indecision or quibble on the part of the users, who are simply expected to act without stopping to consider their options.

The urgency is intended to short-circuit the thinking mind and evoke emotions such as fear, excitement or curiosity. Our survey found that infodemics triggered anxiety and confusion in over 70% of respondents, even if they later identified the messages as fake. This is to show just how strong the appeal of emotionally manipulative language is, and that even users familiar with digital technologies are not immune to it.

The emotional response also applies to the greater likelihood of clicking on malicious hyperlinks or providing sensitive information. For instance, if the message pretends to be from an established organisation such as a bank, social network or government office, people act as if it were real rather than a ruse.

The following is a compilation of common phrases in scam messages and what they are all about. These phrases are deliberately created to tug at our emotions, make us feel urgent or create trust. All of these sentences were constructed to carry out a specific function in making your recipient open the message without questioning the fact that it is legitimate. Analysing the chart will help us to understand how often one type of linguistic tactic occurs in scams and what the possible psychological impact might be on victims.

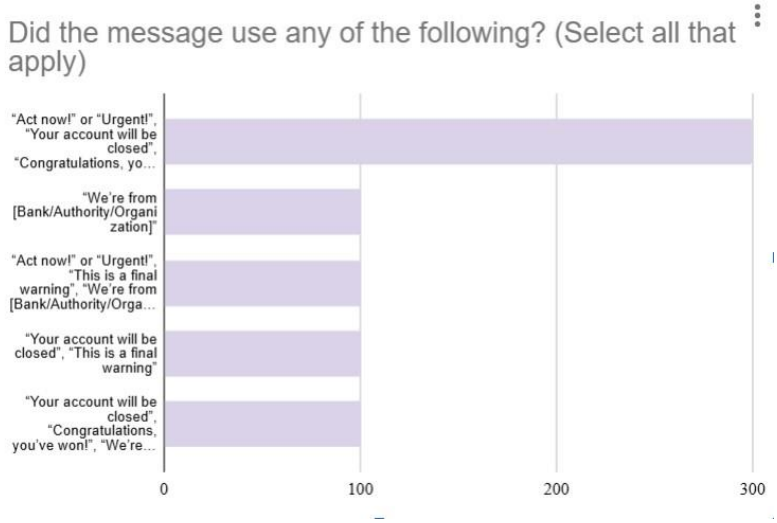


Figure 6: Common Scam Phrases

Language of deception in urgent messages uses certain psychological sub-tactics in order to demand immediate action from the user. Another method to use is time that creates restrictions and limits; it can be a pressure-creating tactic, such as 'Offer expires in 2 hours', or "Your account will be locked in 24 hours." These are meant to provoke an immediate response in order to prevent the user from hesitating as they consider messages like "We've seen some unusual activity mentions." A more common persuasion tactic is fear appeal, where consequences include account deactivation, legal actions or financial loss, as shown by warnings such as "Failure to act will result in account deactivation." Responses to the survey confirmed that these kinds of phrases frequently sparked anxiety or fear and would lead to faster, more careless posting by the users.

Scarcity is also often used alongside limited availability, in ways that can mislead people, such as "Only 2 of these left!" or "Limited stock available", leading people to take action without thinking. Similarly, "Get your gift now – only 50 codes left!" "Once and for all," alerts about disruption are one way of preying on the vulnerability of users to the idea that either their security or their service is at risk. Whether an actual alert or a total invention ("Your recent login from Russia seems suspicious"), scammers are spinning a vivid tale, and a jolt of disbelief and menace can trigger an action in a second. In concert, these strategies combine to bypass conscious reasoning and facilitate superficial responding and are critical in the operation of urgency-based deception.

The result from our poll reveals how cyber criminals deploy language that instils panic in victims. "Confirm your account now" (18.2%) and "Limited time offer! (9.1%) as frequently as suspicious, indicating that scammers create the artificial sense of urgency, thus forcing rushed decisions. And the recent repetition of messages like "Call us immediately" only reinforces this approach of capitalising on fear or excitement to circumvent sobriety of judgment. The statistics emphasise the need to consider such pressure-packed lines as a warning — a potential sign of too-good-to-be-true fraud.

One popular strategy that combines urgency with deception is the "limited-time giveaway" fraud, which often comes with seductive messages like *"Win an iPhone! Only 10 left. First come, first served," or "Congratulations! You have a reward pending!"* This message appeals to both the desire for reward and the fear of missing out (FOMO). By creating a sense of scarcity (*"only 10 left"*) and urgency (*"first come, first served"*), the scammer encourages immediate action without critical thinking (See Appendix B). Typically, clicking the link leads to a phishing site that requests personal details, such as addresses, phone numbers, or even banking information. In many cases, the promise of a prize is completely false, and the user ends up compromising their data or downloading malware.

Studies show that 60 billion spam emails are sent every day, with 46% of the 347 billion daily emails sent considered spam (numbers recorded for 2023) and that the majority of people (96.8%) have received spam messages in some form (Brandl, 2024). The casual yet persuasive tone of these messages contributes to their effectiveness, as it lowers suspicion and creates a sense of authenticity, particularly among individuals who may not be well-versed in recognising digital scams. This linguistic manipulation plays a key role in lowering the user's guard and increasing their susceptibility to fraudulent schemes.

4.2 Exploiting Trust Through Familiar Language

Scammers often mimic the tone of legitimate institutions such as banks, service providers, or even coworkers to appear trustworthy. They use sender addresses or names that closely resemble those of trusted contacts, sometimes differing by just one character. Additionally, they replicate logos, standard greetings, and familiar email templates to reinforce the illusion of authenticity. These small yet calculated choices are designed to lower the recipient's guard and make fraudulent messages appear routine.

Humans are inherently drawn to what feels familiar, a tendency that scammers exploit by using friendly, personalised language that mirrors everyday communication. By addressing recipients by name or using casual, warm tones, scammers create a false sense of connection that reduces scepticism and encourages quick, uncritical responses. To further their deception, scammers employ specific sub-tactics. It is this manipulation that many learned from psychological studies, showing how emotional triggers can bypass the logical mind and cause people to take action that is unplanned action (Academy, 2025). An example of this linguistic engineering is the advance-fee scam email presented in Appendix C.

Scammers make use of additional sub-tactics to enhance their deception. One common method is email spoofing or using lookalike domains—such as support@paypaI.com, where a capital "I" replaces a lowercase "l"—to fool recipients at a glance. In other cases, they reply to old, legitimate email threads to simulate continuity and credibility. These imposters reach out through direct messages, relying on pre-established trust to mislead their targets.

Language in scam messages is often deliberately chosen to evoke trust and provoke action. Research into scam content reveals frequent use of emotionally loaded terms such as "money," "cash," "offer," and "guarantee," which appear consistently across phishing attempts (see Table B1). These words are strategically selected to foster familiarity, urgency, and optimism while minimising suspicion. For example, in 2019, scammers in Karachi targeted retirees by pretending to be bank representatives. People use culturally familiar terms like "uncle" or "auntie" to build rapport and trust. They told the victims that they had urgent problems with their accounts or were giving out promotional rewards and directed them to a spoof banking website. The victims believed that they were talking to actual bank employees and voluntarily presented their personal information, which the scammers used to log into their accounts (Barr, 2024).

4.3 Mimicking Authority: A Strategic Illusion

Scammers often pose as someone with authority, like a bank or a government official, to be taken seriously and to create a sense of urgency. This strategy uses the human propensity to follow perceived authority, which greatly ups the probability of the victim falling for the ruse and losing money. By appearing to be legitimate, scammers can override scepticism and get the recipients to act against their interests.

Many individuals fall for authority-based scams due to a natural tendency to trust people who appear official or knowledgeable. Emotional triggers, such as fear or anxiety, can cloud rational thinking, especially when messages involve threats or urgent consequences. Furthermore, a

widespread lack of awareness and understanding of common digital fraud tactics significantly increases the difficulty for individuals to recognise and respond appropriately to suspicious behaviours, leaving them more vulnerable to deception and exploitation. In societies where authority figures are traditionally respected or obeyed without question, individuals are even less likely to challenge or verify such requests, further enhancing the scam's effectiveness.

To help their mimicking, scammers will try a bunch of techniques. Commonly, they take on professional-sounding titles like "Account Manager," "Security Officer," "Government Agent", – which give them an air of credibility. The messages are drafted in formal tones and filled with legalese to resemble the look of authentic mail. Additionally, scammers create a sense of urgency by using words such as "risk," "bank," and "work" (as seen in Table D1), heightening anxiety and pressuring the target into immediate action.

In 2024, the FBI issued a warning about scammers impersonating FBI agents and other government officials to exploit their perceived authority. These fraudsters claimed the victim was under investigation, using threats of arrest and legal action to pressure them into making immediate payments. By posing as trusted, authoritative figures, the scammers manipulated victims into complying without question. The FBI stressed that federal agencies never demand money through phone calls or emails and advised people to report such incidents to the FBI's Internet Crime Complaint Centre (IC3) (FBI Portland Media Office, 2024).

The following chart illustrates how likely individuals are to trust a message that uses authoritative language and claims to be from an official source, such as formal tone, official logos, or messages that sound important. This data helps assess the effectiveness of these linguistic strategies in convincing people of a message's legitimacy, even when the source may not be trustworthy.

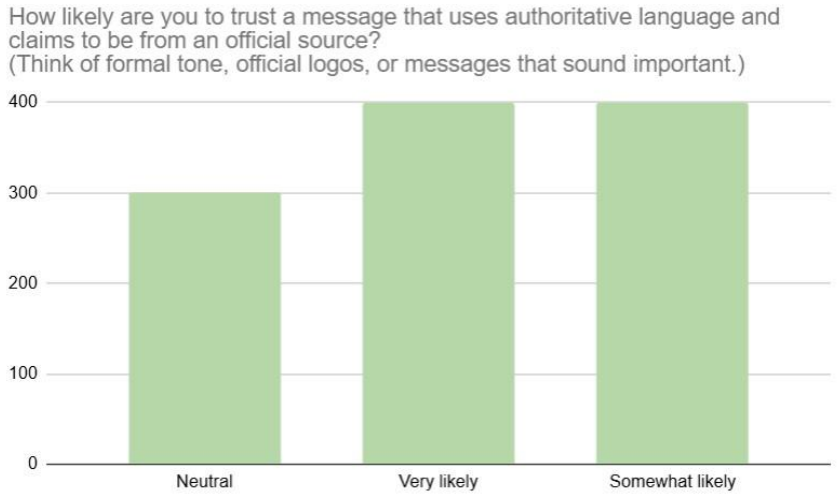


Figure 7: Trust Levels in Messages Using Authoritative Language

Another example of authority-based scamming is illustrated in Appendix C, where a fraudster impersonating the Provincial Director of Union Bank claims to have access to unclaimed funds. Not only does the phoney message offer to pay large sums of money, but it uses language that typically implies it is a legitimate offer. There is a glossary of terms and references, many of which have obscure meanings in the context of financial, commercial or government operations, to bamboozle the reader into believing that mail-outs are genuine.

These messages would often rely on credibility, as this trust in the authority of big institutions such as the Union Bank. People are taught to trust the communication of official entities, and scammers prey on this dependence. By presenting as someone with credibility, scammers lower the potential

victim's scepticism, increasing the likelihood that the victim will follow through and offer personal information, send money or take some similarly nonsensical action. This fraud preys on the natural trust that people place in established organisations, coupled with the belief that well-established institutions would never use them as an accomplice in an illegal operation.

5. Conclusion:

The rise in digital fraud highlights a critical intersection between technology and psychology, particularly in how language can be used to deceive. Hackers and scammers are notoriously precise with their language, and they are not just technically adept; they are word-wise. It is in the language of urgency, faith and authority of the appeals that they make, which circumvent reason as they speak directly to emotion. Whether it's a fake warning letter from a 'bank' or a confirmation email from a household name, the language is deliberately styled to perform the online equivalent of the pickpocketing scam, to encourage hurried, unconsidered responses.

This is effective manipulation because it is a pattern that we connect with legitimacy. When a message is written in the language of the office, mimics the formatting of corporate templates or contains the personalising detail, it is hard to take on faith alone, to not suspect that the sending of it had been against one's interest. These are not technical attacks on a system's weakness, but they are instead a play to the human mind.

By analysing these tactics, we gain insight into how digital threats function beyond code and firewalls. It becomes clear that successful cybercrime often depends more on human behaviour than technical sophistication. Linguistic manipulation reveals why users are so susceptible to clicking hurriedly when fear or urgency or misplaced trust is evoked and why the educated or tech-savvy can still become victims of scams. Some of the psychological ploys used by scammers are of a level beyond common knowledge, pointing to the influence that words and emotions can have on decision-making behaviour.

This dynamic is an important concept not just for cybersecurity specialists but for anyone who engages with computer systems. Accepting that deception is often a matter of a well-crafted message, rather than some sophisticated hack, is the first step to blunting its impact. What we get from the study of language in fraud is not only a warning it's a way of understanding how human interaction and technology are intertwined at a fundamental level. In looking at cyber threats this way, we recognise that defence isn't just about technology, it's also about critical understanding and communications literacy.

5.1 Recommendations:

Educating the public about scam tactics is essential in the fight against digital fraud. Campaigns need to concentrate on these throughout, drawing out the common manipulative strategies, whether the deployment of urgent language or a reliance on authoritative claims that force people to make snap decisions. Drawing attention to important red flags, such as unsolicited requests for personal or financial information, can also aid people in recognising potential threats before it is too late. Finally, the need for a systematic checking of the messages in doubt before execution is pointed out. The campaigns should be issued on multiple channels such as media and community health information programs, which may include social media, television, radio, etc., to reach various populations effectively.

Leveraging the provided tools offers a degree of protection from scams. Email systems can be installed with filters that search for specific words that are typically used in scams, like authoritative or urgent-sounding commands or requests for assistance. Browser extensions can also help defend users by identifying and exposing sites masquerading as reputable entities and warning

right away about phishing campaigns. Automatic security warnings about suspicious contact may also encourage cautiousness and authenticity verification before action.

Understanding how language can be weaponised in the darker digital space can enable people and organisations to fight back, becoming armed warriors against disinformation. We can be inoculated against even the most sophisticated and seductive forms of online deception and fraud by educating and training ourselves, by building technology to detect lies, and by regulating and establishing policy norms.

References

Academy, C. F. (2025). The Psychological Tactics Behind Fraud – How Scammers Exploit Human Behavior. *Canadian Financial Crime Academy*.

Barr, J. D. (2024). Americans older than 60 lost $3.4 billion to scams in 2023: FBI. *ABC News*.

Brandl, C. E. (2024). Spam Statistics 2025: New Data on Junk Email, AI Scams & Phishing. *Emailtooltester*.

Carter, E. (2023). Confirm Not Command: Examining Fraudsters' Use of Language to Compel Victim Compliance in Their Own Exploitation. *British Journal of Criminology* .

Company, B. S. (2022). PA Department of Revenue warns of scam targeting business owners. *Brinker Simpson & Company*.

Daudi, M. (2024). Exploiting Human Trust in Cybersecurity: Which Trust Development Process Is Predominant in Phishing Attacks? *Applied Cybersecurity & Internet Governament*.

Dwivedi, A. (2024). A Comprehensive Review of Phishing in Cybersecurity: Risks, Impacts, and Defence Strategies. *Indian Scientific Journal Of Research In Engineering And Management*.

FBI Portland Media Office. (2024). FBI Warns Public to Beware of Scammers Impersonating FBI Agents and Other Government Officials. *Federal Bureau of Investigation (Portland Field Office)*.

Jimmy, F. (2024). Phishing attackers: prevention and response strategies. *Journal of Artificial Intelligence & Global Security*, 307-318.

Kutub Thakur, . (2023). A Systematic Review on Deep-Learning-Based Phishing Email Detection. *Electronics* , Vol. 12, Issue 21, Article 4545.

Lauren E. Scissors, A. J. (2008). Linguistic mimicry and trust in text-based CMC. *Conference on Computer Supported Cooperative Work*, 277-280.

Lawson, P. A., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*.

Liu, B. G. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. *Electronics*, Article 1671.

mukti, s. (2024). Urgent warning scam alert ahead vector design.

Scamwatch. (2024). Scam statistics. *Scamwatch (ACCC / National Anti-Scam Centre)*.

Suela, L. C. (2024). Online Fraud Exposed: Tactics and Strategies of Cyber Scammers. *Indian Scientific Journal Of Research In Engineering And Management* .